KRSC
مركز الكويت للبحوث والدراسات
KUWAIT RESEARCH AND STUDIES CENTER

مركز الخليج للأبحاث
المعرفة للجميع
Gulf Research Center
Knowledge for All

سيادة البيانات والاستقلال الاستراتيجي في الخليج

ورقة سياسات

د. زينب أشكناني
قسم الهندسة الحيوية والزراعية ومعهد الطاقة
جامعة تكساس إي أند إم، الولايات المتحدة الأمريكية

الملخص التنفيذي

تسعى دول مجلس التعاون لدول الخليج العربية إلى التحول إلى مراكز عالمية للذكاء الاصطناعي والحوسبة السحابية، بالتوازي مع تأكيد سيادتها الوطنية على بنيتها التحتية الرقمية. غير أن الجمع بين هذين الطموحين يخلق توترًا لم يُحسم بعد. وتشير الإعلانات العامة إلى استثمارات تتجاوز ٣٠ مليار دولار أمريكي في مراكز بيانات الذكاء الاصطناعي في دول المجلس بحلول عام ٢٠٣٠ (Analysys Mason ٢٠٢٥). ومع ذلك، يُبنى جزء كبير من هذه القدرة ويُشغَّل بالشراكة مع مزوّدي خدمات سحابية أجانب فائقي النطاق، تظل منتجاتهم خاضعة لقوانين تتجاوز الحدود الوطنية، مثل قانون CLOUD الأمريكي (U.S. Congressional Research Service ٢٠١٨). وينشأ عن ذلك ما يمكن وصفه بمفارقة السيادة: فالمنطقة تبني البنية المادية للاستقلال الرقمي اعتمادًا على منظومة من البرمجيات والنماذج وسلاسل التوريد لا تزال خارج سيطرتها.

> **تسعى دول مجلس التعاون لدول الخليج العربية إلى التحول إلى مراكز عالمية للذكاء الاصطناعي والحوسبة السحابية**

تقيّم هذه الورقة واقع سيادة البيانات في دول مجلس التعاون، وتحدد الفجوات التنظيمية والمؤسسية، وتبحث المخاطر الاستراتيجية الناجمة عن استمرار الاعتماد على الخارج، وتطرح سبع توصيات لصنّاع القرار الراغبين في تعزيز الحماية الوطنية للبيانات وضمان التبني المسؤول للتقنيات المتقدمة، من دون التضحية بالانفتاح الذي يدعم الابتكار والاستثمار الأجنبي ونقل المعرفة.

وتنطلق الورقة من حجة رئيسية مفادها أن السيادة في العصر الرقمي لا ينبغي أن تُفهم بوصفها خيارًا ثنائيًا بين الانفتاح والسيطرة، بل باعتبارها سلسلة من القرارات المقصودة بشأن الطبقات التي يجب أن تتركز فيها السيطرة الوطنية ضمن المنظومة التقنية. فالاستضافة المادية للبيانات لا توفر، بمفردها، حماية تُذكر عندما تظل البرمجيات ومفاتيح التشفير والمعالجات والنماذج التي تعمل فوقها خاضعة لسيطرة أجنبية. وتتمتع دول الخليج بعدة مزايا نسبية، من بينها وفرة رأس المال، وسرعة اتخاذ القرار السياسي، ومحدودية القيود الناجمة عن الأنظمة التقنية القديمة، وتنافسية تكاليف الطاقة. وتتيح هذه المزايا للمنطقة اتخاذ مثل هذه القرارات بسرعة تفوق كثيرًا من المناطق الأخرى. ولا يتمثل الخطر في عجز الخليج عن بناء القدرات، بل في أن يتحدد موضع السيطرة ضمنيًا من خلال قرارات الشراء وخطط المورّدين، بدلًا من أن تحدده استراتيجية وطنية واضحة.

١

ضرورة السيادة

تعني سيادة البيانات أن تخضع البيانات المُنتجة داخل دولة أو نطاق قانوني معين لقوانين تلك الدولة ورقابتها وحمايتها. وبالنسبة إلى الدول التي تسعى إلى تسريع تحولها الرقمي، لم تعد السيادة مفهومًا قانونيًا مجردًا، بل أصبحت قضية استراتيجية تمس الأمن الوطني والتنافسية الاقتصادية وثقة المواطنين.

وقد جعلت ثلاثة تطورات هذه القضية أكثر إلحاحًا. أولًا، نقلت ثورة الذكاء الاصطناعي مركز ثقل القوة الوطنية من البنية التحتية المادية إلى البنية التحتية الرقمية؛ إذ أصبحت القدرة الحوسبية، وبيانات التدريب، وأوزان النماذج، والكفاءات القادرة على تشغيلها، من بين أكثر الموارد أهمية استراتيجية. ثانيًا، ازداد المشهد الجيوسياسي انقسامًا. فقد أظهرت المنافسة بين الولايات المتحدة والصين، والقيود المفروضة على تصدير أشباه الموصلات المتقدمة، وتطبيق أنظمة قانونية عابرة للحدود مثل قانون CLOUD، أن الخدمات السحابية «العالمية» تخضع عمليًا لقوانين الدولة التي ينتمي إليها مزوّد الخدمة (U.S. Congressional Research Service ٢٠١٨). ثالثًا، تنتج مجتمعات الخليج كميات متزايدة من بيانات المواطنين والبيانات المالية والأمنية الحساسة، وهو ما يرفع كلفة أي اختراق أو إفصاح قسري عنها.

ومن المهم التمييز بين سيادة البيانات والمفاهيم الأوسع التي كثيرًا ما تختلط بها. فسيادة البيانات تتعلق بالنطاق القانوني الذي يحكم مجموعات بيانات محددة. أما السيادة الرقمية فتمتد إلى البرمجيات والمنصات والمعايير التي تُخزَّن البيانات وتُعالَج من خلالها. وتأتي السيادة التكنولوجية في نطاق أوسع، إذ تشمل القدرة على تصميم الأجهزة وتصنيعها وتدريب النماذج محليًا. وقد تنجح دولة ما في تأمين المستوى الأول، بينما تظل معتمدة كليًا على الخارج في المستويين الثاني والثالث، وهو ما يصف إلى حد بعيد الوضع الراهن في الخليج. لذلك، لا يتمثل السؤال العملي أمام صنّاع السياسات في السعي إلى سيادة مطلقة، بل في تحديد مجموعات البيانات وأحمال العمل والقدرات التي تُعد استراتيجية بما يكفي لتبرير كلفة إخضاعها لسيطرة وطنية فعلية، وتحديد ما يمكن تركه لأسواق دولية مفتوحة وتنافسية.

٢.

المشهد الراهن: طموح كبير واعتماد مستمر

استجابت حكومات دول مجلس التعاون من خلال مزيج من التنظيم، والبنية التحتية السيادية، والاستثمار الاستراتيجي.

تمثلت الاستجابة الأولى في تطوير الأطر التنظيمية. فقد فرض نظام حماية البيانات الشخصية في المملكة العربية السعودية (PDPL)، الذي تشرف عليه الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) ومكتب إدارة البيانات الوطنية (NDMO)، متطلبات لتوطين نطاق واسع من البيانات الشخصية والحكومية (Saudi Data and Artificial Intelligence Authority ٢٠٢١). كما أصدرت دولة الإمارات مبادئ توجيهية لأخلاقيات الذكاء الاصطناعي، وقوانين اتحادية لحماية البيانات، وأنظمة خاصة بالمناطق الحرة، مثل سوق أبو ظبي العالمي ومركز دبي المالي العالمي، تتيح حوكمة البيانات وفق أطر مستندة إلى القانون العام ("AI and Data Protection Regulation" ٢٠٢٥). وتؤكد الاستراتيجية الوطنية للأمن السيبراني في قطر ٢٠٢٤–٢٠٣٠ أهمية التعامل السيادي مع البيانات (Government Communications Office ٢٠٢٤)، فيما كان قانون حماية البيانات الشخصية البحريني لعام ٢٠١٨ أول إطار شامل من نوعه في المنطقة (DLA Piper, n.d.). كما ينظم القرار الوزاري العُماني رقم ٢٠٢٤/١١٥٢ خدمات الحوسبة السحابية ومراكز البيانات، ويقيّد نقل البيانات الحساسة عبر الحدود (Telecommunications Regulatory Authority ٢٠٢٤). وفي الكويت، تتبلور الاستراتيجية الوطنية للذكاء الاصطناعي بالتوازي مع قواعد سيبرانية جديدة صادرة عن بنك الكويت المركزي (Chambers and Partners ٢٠٢٥).

أما الاستجابة الثانية فتمثلت في بناء بنية تحتية سيادية مدعومة باستثمارات واسعة. فقد أطلقت السعودية شركة HUMAIN مطلع عام ٢٠٢٥ بوصفها كيانًا وطنيًا رائدًا يستثمر عبر سلسلة قيمة الذكاء الاصطناعي (Analysys Mason ٢٠٢٥)، وأعلنت المملكة استثمارات تتجاوز ١٨ مليار دولار في مراكز البيانات ضمن رؤية ٢٠٣٠ (Ministry of Communications and Information Technology, n.d.)، من بينها مجمع «أوكساغون» المخطط له في نيوم بقدرة ١,٥ غيغاواط (NEOM ٢٠٢٥). وفي الإمارات، تقود مجموعة G٤٢ مشروع «ستارغيت الإمارات» بقيمة ٢٠ مليار دولار، وهو منشأة فائقة النطاق مخصصة

للذكاء الاصطناعي بقدرة ٥ غيغاواط، ومصممة لاستضافة ما يصل إلى ٢٫٥ مليون وحدة معالجة رسومات، بالشراكة مع OpenAI وNvidia وOracle وSoftBank (Sophia ٢٠٢٥; OpenAI ٢٠٢٥). ويُعد هذا أول موقع دولي لـOpenAI. كما أعلنت Microsoft توسعًا بقيمة ٧٫٩ مليار دولار عبر مراكز بيانات «خزنة» خلال الفترة ٢٠٢٦–٢٠٢٩ (Data Center Dynamics ٢٠٢٥a). وأطلقت شركة Syntys التابعة لـ Ooredoo في قطر سحابة سيادية للذكاء الاصطناعي مدعومة باستثمار قدره مليار دولار (Data Center Dynamics ٢٠٢٥c). وفي البحرين، تستثمر شركتا stc وcenter٣ نحو ٣٢٠ مليون دولار في مجمع البحرين لمراكز البيانات وكابل «Pearls ٢Africa» البحري (Analysys Mason ٢٠٢٥). أما الكويت، فقد حصلت على التزامات من Cloud Google وAzure Microsoft بإنشاء مناطق سحابية محلية داخل البلاد (Data Center Dynamics ٢٠٢٥b).

عمليًا، يشمل مصطلح «السحابة السيادية» ترتيبات متعددة تختلف بدرجة كبيرة في مستوى السيطرة الذي تتيحه. ففي أحد طرفي هذا الطيف توجد مناطق سحابية عالمية تقع ماديًا داخل الدولة، لكنها تُشغَّل وتُدار وتخضع قانونيًا للمزوّد الأجنبي. وفي الوسط توجد نماذج الشراكة والامتياز، حيث يحتفظ كيان محلي بالترخيص ويعيّن موظفين وطنيين خضعوا للتدقيق الأمني، بينما تُدار المنشأة باستخدام تقنيات المزوّد. وفي الطرف الآخر توجد أنظمة معزولة شبكيًا بصورة كاملة، منفصلة عن شبكة المزوّد وتُشغَّل بالكامل بواسطة كوادر محلية. وتتركز معظم المشروعات الخليجية الحالية في الفئتين الأوليين؛ فهي تحقق فوائد فعلية في توطين البيانات وتقليل زمن الاستجابة، لكنها تُبقي قدرًا كبيرًا من السيطرة التشغيلية والقانونية في يد المزوّد. ولذلك، فإن تحديد موقع كل عبء عمل على هذا الطيف، والموقع الذي ينبغي أن يشغله، شرط أساسي لاتخاذ قرارات شراء سليمة.

وعلى الرغم من ضخامة هذه الاستثمارات، تستمر ثلاثة مستويات رئيسية من الاعتماد. أولًا، منظومة الحوسبة السحابية فائقة النطاق؛ إذ تُشغِّل AWS وMicrosoft وOracle وGoogle وHuawei معظم ما يُسمى بالمناطق السحابية السيادية، وفق نماذج امتياز أو شراكة (ResearchAndMarkets ٢٠٢٥). ثانيًا، طبقة القدرة الحوسبية؛ تُنتج وحدات معالجة الرسومات المتقدمة شركات Nvidia وAMD و TSMC، وتظل خاضعة لقيود التصدير الأمريكية (Data Center World Middle East ٢٠٢٦). ثالثًا، طبقة النماذج؛ لا تزال النماذج التأسيسية الرائدة تُطوَّر أساسًا في الولايات المتحدة والصين (Computer Weekly ٢٠٢٦). ومن ثم، فإن توطين الأجهزة داخل مركز بيانات خليجي لا يعني، في حد ذاته، توطين السيطرة.

٣.
الفجوات التنظيمية والمؤسسية

تعاني الأطر الحالية من خمس نقاط ضعف هيكلية.

تتمثل الأولى في تشتت الأطر بين دول مجلس التعاون. فلكل دولة من الدول الست سلطة مستقلة لحماية البيانات، وهيئات تنظيمية قطاعية منفصلة، مثل البنك المركزي السعودي، ومصرف الإمارات المركزي، ومصرف قطر المركزي، ومصرف البحرين المركزي، وبنك الكويت المركزي، والبنك المركزي العُماني (Saudi Central Bank, n.d.)، فضلًا عن أنظمة مختلفة لتصنيف البيانات. ولذلك، تواجه البنوك والمستشفيات والجهات الحكومية التي تعمل إقليميًا ستة أنظمة امتثال متداخلة، من دون آلية للاعتراف المتبادل تماثل قرارات كفاية الحماية في الاتحاد الأوروبي. ويرفع ذلك الكلفة، ويحد من الخدمات الرقمية العابرة للحدود، ويضعف القدرة التفاوضية الجماعية لدول المجلس في مواجهة مزوّدي الخدمات السحابية الأجانب فائقي النطاق.

> **“تواجه البنوك والمستشفيات والجهات الحكومية التي تعمل إقليميًا ستة أنظمة امتثال متداخلة من دون آلية للاعتراف المتبادل تماثل قرارات كفاية الحماية في الاتحاد الأوروبي**

أما الثانية فهي بطء التنفيذ، فكثيرًا ما تكون القوانين متقدمة على مستوى النص، لكنها محدودة التطبيق في الممارسة. ولم تواكب الموارد والقدرات التقنية وبنى التدقيق المتاحة لسلطات حماية البيانات الوطنية حجم أنشطة المعالجة الخاضعة للتنظيم وتعقيدها، ولا سيما في تدريب نماذج الذكاء الاصطناعي ونقل البيانات عبر الحدود.

وتتمثل الثالثة في التعرض لقوانين وسلطات أجنبية عابرة للحدود. فحتى البيانات المخزنة ماديًا في الخليج قد تُلزم الجهات المشغلة بتسليمها إلى سلطات أجنبية متى كانت خاضعة لنطاقها القانوني. ويتيح قانون CLOUD الأمريكي إلزام مزوّدي الخدمات الأمريكيين بتقديم البيانات الواقعة في حيازتهم أو عهدتهم أو سيطرتهم بصرف النظر عن موقعها المادي (U.S. Congressional Research Service ٢٠١٨). كما أبرزت قضية الكشف عن مفاتيح BitLocker في عام ٢٠٢٥ أن مفاتيح التشفير التي يحتفظ بها المزوّد

يمكن الوصول إليها من خلال إجراءات قانونية (Constantin ٢٠٢٦). ولم تطوّر دول المجلس بعد متطلبات كافية للتشفير، والحيازة الوطنية لمفاتيح التشفير، والحوسبة السرية، بما يحد من هذا التعرض.

أما الرابعة فهي محدودية قاعدة الابتكار المحلية، إذ لا يزال الإنفاق على البحث والتطوير في معظم دول المجلس دون ١ في المائة من الناتج المحلي الإجمالي، فيما تتصدر الإمارات إقليميًا بنسبة تقارب ١,٥ في المائة، وهي أقل بكثير من متوسط منظمة التعاون الاقتصادي والتنمية البالغ ٢,٦ في المائة (World Bank, n.d.). ومن دون قاعدة محلية أقوى للبحث والكفاءات، قد تتحول البنية التحتية السيادية إلى واجهة تقنية متقدمة تخفي اعتمادًا مستمرًا على قدرات مستوردة.

وتتمثل الخامسة في غياب التنسيق في المشتريات، فعلى المستوى الجماعي، تُعد حكومات دول مجلس التعاون من أكبر مشتري خدمات الحوسبة السحابية والذكاء الاصطناعي في الأسواق الناشئة، لكنها نادرًا ما توظف هذه القوة الشرائية بصورة منسقة. ولا يوجد نظام اعتماد مشترك يُعتمد بموجبه المزوّد مرة واحدة ثم يُعترف به في الأسواق الستة، كما لا توجد قاعدة موحدة للشروط التعاقدية المتعلقة بالوصول إلى البيانات، والمعالجة من الباطن، وقابلية نقل البيانات، والخروج من الخدمة، والإبلاغ عن الاختراقات. ونتيجة لذلك، تتفاوض كل جهة من موقع أضعف مما يبرره حجم الإنفاق الخليجي الإجمالي، ولا يواجه المزوّدون ضغطًا كافيًا لتحسين شروطهم العالمية المعتادة. ومن شأن إنشاء نظام منسق للمشتريات والاعتماد، يجمع بين متطلبات أمنية أساسية مشتركة والاعتراف المتبادل بالمزوّدين المعتمدين، أن يحوّل الطلب الوطني المتفرق إلى قوة تفاوضية جماعية مؤثرة.

٤.
المخاطر الاستراتيجية

هناك خمسة مخاطر تستحق اهتمامًا خاصًا من صنّاع السياسات.

أولها، قابلية الاعتماد التقني للتحول إلى أداة ضغط جيوسياسي. فقد تتعطل أحمال العمل الحيوية المعتمدة على دولة أجنبية واحدة بفعل قيود التصدير أو العقوبات أو الضغوط السياسية. كما أظهرت النزاعات الإقليمية الأخيرة أن الأصول المادية لمراكز البيانات ليست محصنة من مخاطر الاستهداف العسكري أو الأضرار المادية المباشرة.

وثانيها، الارتهان التقني الذي يقيّد الابتكار. فقرارات الشراء المتخذة اليوم لصالح منظومات ذكاء اصطناعي ونماذج وواجهات برمجة تطبيقات وأطر للوكلاء الذكية مملوكة لجهات أجنبية تخلق تكاليف انتقال تتزايد بمرور الوقت، وتحد من خيارات السياسات مستقبلًا.

وثالثها، ما يتعلق بثقة المواطنين وحقوقهم. فعندما تصبح البيانات الحساسة، بما فيها الصحية والبيومترية والمالية والأمنية، عرضة لإجراءات قانونية أجنبية، لا تستطيع الحكومات أن تضمن بصورة ذات صدقية التزامات الخصوصية المنصوص عليها في الدساتير والقوانين الوطنية.

ورابعها، تسرب القيمة الاقتصادية إلى الخارج. فمن دون قدرات سيادية في النماذج والبرمجيات والخدمات، قد يتحول الخليج إلى مجرد مستضيف للبنية التحتية الحوسبية، بينما تذهب معظم عوائدها الاقتصادية إلى المزوّدين وأصحاب التراخيص الأجانب.

وخامسها، التركّز والهشاشة النظامية. تجذب الشراكات مع المزوّدين فائقي النطاق بسبب وفورات الحجم، والتكامل العميق بين الأدوات، وسرعة النشر. غير أن هذه المزايا نفسها تركز النشاط الرقمي الوطني في عدد محدود من المزوّدين والمواقع المادية. ولذلك، قد يمتد أثر خطأ واحد في الإعداد، أو انقطاع طويل، أو حادث سيبراني، أو نزاع تجاري، إلى قطاعات المصارف والخدمات الحكومية والرعاية الصحية والاتصالات في آن واحد. وتتعامل الجهات التنظيمية في دول أخرى بصورة متزايدة مع هذا النوع من التركّز بوصفه مسألة تتعلق بالاستقرار النظامي، لا مجرد قرار شراء اعتيادي؛ فتفرض على المؤسسات الخاضعة لإشرافها متطلبات لإدارة مخاطر التركّز ووضع خطط للخروج من الخدمات (European Insurance and Occupational Pensions Authority, n.d.). وبالنسبة إلى اقتصادات الخليج التي تقوم استراتيجيات تنويعها صراحة على البنية التحتية الرقمية، تستحق كلفة الهشاشة الناجمة عن الاعتماد على مزوّد واحد أو منطقة واحدة مستوى التدقيق ذاته الذي خضع له طويلًا الاعتماد المفرط على سلعة تصديرية واحدة.

٥،
نماذج دولية مرجعية

ليست منطقة الخليج أول من يواجه هذه المفاضلات. وتقدم أربعة نماذج دولية مقارنات مفيدة.

بنى الاتحاد الأوروبي سيادته الرقمية في المقام الأول من خلال القانون، عبر قرارات كفاية الحماية بموجب اللائحة العامة لحماية البيانات، وحكم Schrems II، وقانون حوكمة البيانات، وقانون الذكاء الاصطناعي (World Economic Forum ٢٠٢٥). وتوفر قرارات الكفاية نموذجًا مفيدًا للآلية الخليجية المقترحة أدناه، إلا أن التجربة الأوروبية توضح أيضًا حدود السيادة القانونية في غياب بنية تحتية مستقلة؛ إذ تظل أحمال العمل الأوروبية الحيوية معتمدة بدرجة كبيرة على مزوّدي الخدمات السحابية الأمريكيين فائقي النطاق، رغم مبادرة X-Gaia وغيرها (The Next Web ٢٠٢٦).

أما الصين، فقد بنت سيادتها أساسًا من خلال البنية التحتية والملكية، عبر سوق سحابية محلية تهيمن عليها Alibaba وTencent وHuawei وBaidu (Information Technology and Innovation Foundation, n.d.)، وقواعد صارمة لتصدير البيانات بموجب قانون الأمن السيبراني وقانون أمن البيانات وقانون حماية المعلومات الشخصية (Foreign Policy ٢٠٢٢)، ونهج يقوم على منظومة مغلقة لنماذج الذكاء الاصطناعي. وقد نتج عن ذلك استقلال مستدام، لكن بكلفة تتمثل في زيادة الاحتكاك مع التجارة الرقمية العالمية وتراجع تدفقات التكنولوجيا والكفاءات الأجنبية.

> **تظل أحمال العمل الأوروبية الحيوية معتمدة بدرجة كبيرة على مزوّدي الخدمات السحابية الأمريكيين فائقي النطاق**

واتبعت الهند مسارًا وسطًا. فقد أبقى قانون حماية البيانات الشخصية الرقمية لعام ٢٠٢٣ تدفقات البيانات العابرة للحدود مفتوحة نسبيًا (Hogan Lovells ٢٠٢٥)، بالتوازي مع بناء طبقة سيادية من البنية التحتية الرقمية العامة، تشمل Aadhaar وUPI وONDC، تتسم بالانفتاح والطابع العام والحوكمة المحلية (Center for Strategic and International Studies, n.d.). وتشير التجربة الهندية إلى إمكان بناء السيادة على مستوى البروتوكولات، وليس فقط على مستوى مراكز البيانات.

ولعل سنغافورة تقدم النموذج الأقرب إلى وضع الخليج: اقتصاد صغير غني برأس المال ومعتمد على التجارة، سعى إلى الريادة الرقمية مع إبقاء أبوابه مفتوحة بدرجة كبيرة أمام التكنولوجيا ورأس المال والكفاءات الأجنبية. وقد جمعت سنغافورة بين نظام عملي لحماية البيانات بموجب قانون حماية البيانات الشخصية (International Association of Privacy Professionals, n.d.) وأدوات إرشادية غير ملزمة لكنها مؤثرة، مثل الإطار النموذجي لحوكمة الذكاء الاصطناعي (Duane Morris & Sel-vam ٢٠٢٦). كما وضعت نفسها مركزًا موثوقًا لمراكز البيانات والاتصال عبر الكابلات البحرية، بدلًا من السعي إلى امتلاك جميع طبقات المنظومة محليًا. وتركز استراتيجيتها على المصداقية التنظيمية، وقابلية التشغيل البيني، والمشاركة النشطة في وضع المعايير، أكثر من تركيزها على الاكتفاء الذاتي؛ أي ممارسة السيادة من خلال الثقة وجودة المؤسسات بقدر ممارستها من خلال السيطرة على الأجهزة. وبالنسبة إلى دول الخليج، التي تتشابه معها في الحجم والانفتاح، تبدو عناصر عدة من هذا النهج أكثر قابلية للتطبيق من النماذج الأوروبية أو الصينية أو الهندية.

لا يمكن نقل أي من هذه النماذج إلى الخليج بصورة مباشرة، وإن كانت سنغافورة الأقرب. فمحدودية عدد السكان، ووفرة رأس المال، والانفتاح على الخبرات الأجنبية، عوامل لا تتناسب مع النموذج الصيني. كما أن القدرات التنظيمية التي لا تزال في طور النضج تحد من إمكان الاعتماد الكامل على النموذج الأوروبي، فيما تختلف بنية الاقتصاد السياسي الخليجي جوهريًا عن الهند. ومن ثم، يلائم الخليج نهج هجين يجمع بين الاستثمار الانتقائي في البنية التحتية، والتوطين القانوني الموجّه، والمشاركة النشطة في صياغة المعايير الدولية.

٦.

توصيات السياسات

تهدف التوصيات السبع الآتية إلى تعزيز السيادة من دون التضحية بالانفتاح أو الشراكات أو الابتكار.

أولًا، اعتماد معيار إقليمي متدرج لتصنيف البيانات على مستوى دول مجلس التعاون. واستنادًا إلى الجهود الوطنية، ولا سيما تصنيفات مكتب إدارة البيانات الوطنية السعودي (Saudi Data and Artificial Intelligence Authority ٢٠٢١)، ينبغي للأمانة العامة لمجلس التعاون رعاية نظام موحد من أربع درجات: بيانات عامة، وداخلية، وسرية، وسيادية. ويُربط كل مستوى بنموذج استضافة مسموح به: منطقة سحابية عالمية فائقة النطاق، أو منطقة فائقة النطاق داخل الدولة، أو سحابة سيادية، أو نظام سيادي معزول شبكيًا. ومن شأن ذلك خفض أعباء الامتثال من دون إضعاف مستوى الحماية.

ثانيًا، إلزام أحمال العمل المصنفة سيادية بالحيازة الوطنية لمفاتيح التشفير واستخدام الحوسبة السرية. وينبغي معالجة بيانات المواطنين والأمن والقطاع المالي شديدة الحساسية ضمن بنى تحتفظ فيها جهات وطنية وحدها بمفاتيح التشفير، ويفضل أن تكون مدعومة بحوسبة سرية مفروضة على مستوى الأجهزة. كما ينبغي أن تلزم معايير الشراء المزوّدين الأجانب بإثبات عجزهم البنيوي عن الوصول إلى البيانات بصيغتها غير المشفرة.

ثالثًا، إنشاء آلية خليجية للاعتراف بتكافؤ مستوى حماية البيانات. فمن شأن إطار للاعتراف المتبادل، مستوحى بصورة عامة من قرارات كفاية الحماية في الاتحاد الأوروبي، أن يسمح بالتدفق الحر للبيانات الشخصية بين دول المجلس التي تُعد أطرها متكافئة، بما يقلل ازدواجية المتطلبات على المشغلين الإقليميين، مع الحفاظ على السيادة في التعامل مع الأطراف الخارجية.

رابعًا، الاستثمار في طبقة سيادية للنماذج والأدوات. فإلى جانب مراكز البيانات، ينبغي توجيه الاستثمار العام إلى النماذج التأسيسية باللغة العربية، والبنية اللازمة للضبط الدقيق، وقدرات التقييم، والمساهمات في البرمجيات مفتوحة المصدر. كما ينبغي تنسيق مبادرات HUMAIN و G٤٢ و Falcon وغيرها، بدلًا من تكرارها، وربطها بأفضلية في المشتريات المتعلقة بأحمال العمل الحكومية (Computer Weekly ٢٠٢٦).

خامسًا، بناء مسار مستدام لتنمية الكفاءات. ويمكن تحقيق ذلك عبر توسيع برامج مثل أكاديمية مراكز البيانات السعودية (Uptime Institute ٢٠٢٤) ومبادرات تدريب المبرمجين في الإمارات، وزيادة تمويل برامج الدكتوراه في سلامة الذكاء الاصطناعي والتشفير، وإنشاء برامج إعارة وتبادل مهني على مستوى دول المجلس بين الجهات التنظيمية والمشغلين. ومن شأن ذلك الحد من الاعتماد على الخبرات المستوردة الذي يضعف حاليًا صدقية الادعاءات بالسيادة.

سادسًا، الحفاظ على انفتاح محسوب. ينبغي قصر متطلبات توطين البيانات على الفئات الحساسة فعلًا، واستخدام أنظمة المناطق الحرة، مثل سوق أبو ظبي العالمي ومركز دبي المالي العالمي ونيوم، بوصفها مختبرات للسياسات تستطيع فيها الشركات الدولية العمل وفق قواعد واضحة وقابلة للإنفاذ. فالهدف هو فرض سيطرة انتقائية على المجالات الأكثر أهمية، لا تبني الانغلاق أو الاكتفاء الذاتي الكامل.

سابعًا، اضطلاع دول الخليج بدور قيادي في المعايير الدولية ودبلوماسية التجارة الرقمية. فسيادة الاقتصادات الصغيرة والمفتوحة تُمارس من خلال التأثير في القواعد بقدر ما تُمارس من خلال امتلاك الأصول. وينبغي لدول المجلس تنسيق مشاركتها في هيئات المعايير الدولية، ومنتديات حوكمة الذكاء الاصطناعي، وترتيبات تدفق البيانات عبر الحدود، والسعي إلى اتفاقيات متبادلة للاعتراف بكفاية الحماية مع الشركاء الرئيسيين، بما يضمن تمتع البيانات المستضافة في الخليج بحماية معترف بها خارج المنطقة. كما أن الاستثمار في القدرات الدبلوماسية والتقنية اللازمة للمساهمة في صياغة المعايير الناشئة المتعلقة بتقييم النماذج، والنقل القانوني للبيانات عبر الحدود، واعتماد أمن الخدمات السحابية، سيضع المنطقة في موقع صانع القواعد، لا المتلقي لها. وإذا نُفذ ذلك بفاعلية، فسوف يعزز القوة التفاوضية الناجمة عن استثمارات المنطقة في البنية التحتية، ويحوّل المصداقية التنظيمية إلى عامل جذب للبيانات الموثوقة والشراكات والاستثمارات.

الخلاصة

تمتلك دول الخليج رأس المال والإرادة السياسية والطموح في مجال البنية التحتية بما يؤهلها لقيادة اقتصادات الذكاء الاصطناعي في الأسواق الناشئة. غير أن تحويل هذه الريادة إلى استقلال استراتيجي مستدام سيتوقف بدرجة أقل على عدد غيغاواطات القدرة الحوسبية التي تنشرها، وبدرجة أكبر على المؤسسات والأطر والقدرات البشرية التي تبنيها حول تلك البنية. فالسيادة في العصر الرقمي ليست جدارًا، بل بنية متعددة الطبقات تتكون من القوانين ومفاتيح التشفير والكفاءات والشراكات. ويتمثل التحدي المركزي للسياسات خلال العقد المقبل في تصميم هذه البنية بصورة مقصودة، بدلًا من تركها تتشكل باعتبارها نتيجة ثانوية لقرارات المزوّدين.

> **“السيادة في العصر الرقمي ليست جدارًا، بل بنية متعددة الطبقات تتكون من القوانين ومفاتيح التشفير والكفاءات والشراكات**

وسيتطلب تحويل هذه البنية إلى واقع عملي ترتيبًا واضحًا للأولويات وتسلسلًا في التنفيذ بقدر ما يتطلب طموحًا. وينبغي البدء بثلاث أولويات: معيار موحد لتصنيف البيانات، ومتطلبات للحيازة الوطنية لمفاتيح التشفير الخاصة بأكثر أحمال العمل حساسية، وآلية للاعتراف المتبادل بين دول مجلس التعاون. وهذه أولويات مؤسسية إلى حد كبير، ويمكن تطويرها بالتوازي مع العمل الأطول أمدًا لبناء نماذج سيادية وقاعدة محلية للكفاءات، بدلًا من انتظار اكتمال ذلك العمل. وينبغي قياس التقدم بمؤشرات ملموسة، من بينها نسبة البيانات المصنفة سيادية التي تخضع لحيازة وطنية حصرية لمفاتيح التشفير، ونسبة أحمال العمل الحكومية الحيوية التي تخدمها قدرات إقليمية منسقة، وتنوع المزوّدين الذين تعتمد عليهم الخدمات الأساسية، ونمو الإنتاج البحثي المحلي والوظائف عالية المهارة. ووفق هذه المؤشرات، تصبح السيادة أقل شبهًا بهدف يُعلن الوصول إليه، وأكثر شبهًا بممارسة مؤسسية يجب الحفاظ عليها باستمرار.

المراجع

1. AI and Data Protection Regulation: What Businesses Need to Know." ٢٠٢٥. UAE PDPL," Federal Decree–Law No. ٤٥ of ٢٠٢١; DIFC Data Law; ADGM Data Protection Regulations. Lexology. https://www.lexology.com/library/detail.aspx?g=٣fa٦٦٣c٦–bb٢١–٤eld–alc٤–٤٦٣e٤c٨٠٠٥٢a

2. Analysys Mason. ٢٠٢٥. "AI Investment in the GCC: Accelerated Investment in AI Data Centres Will Reach USD ٥–٧ Billion in ٢٠٢٦." Predictions ٢٠٢٦. https://www.analysysma-/son.com/about–us/news/predictions–٢٠٢٦/prediction–ai–investment–gcc

3. Center for Strategic and International Studies (CSIS). n.d. "Ten Years of UPI: Implications of India's Digital Public Infrastructure for Data Protection." https://www.csis.org/blogs/strategic–technologies–blog/ten–years–upi–implications–indias–digital–public–infrastructure

4. Chambers and Partners. ٢٠٢٥. "Kuwait's AI Revolution: Law, Cloud, and Cybersecurity at the Core of Digital Transformation." https://chambers.com/articles/kuwait–s–ai–revolution–law–cloud–and–cybersecurity–at–the–core–of–digital–transformation

5. Computer Weekly. ٢٠٢٦. "UAE's TII Challenges Big Tech Dominance with Open Source Falcon AI Models." https://www.computerweekly.com/news/٣٦٦٦٣٨٧٥٩/UAEs–TII–challenges–big–tech–dominance–with–open–source–Falcon–AI–models

6. Constantin, Lucian. ٢٠٢٦. "Microsoft Handed Over BitLocker Keys to Law Enforcement, Raising Enterprise Data Control Concerns." CSO Online, January. https://www.csoonline.com/article/٤١٢٢١٥١/microsoft–handed–over–bitlocker–keys–to–law–enforcement–raising–enterprise–data–control–concerns–٢.html

7. Data Center Dynamics. ٢٠٢٥a. "Microsoft and G٤٢ Expand Data Center Capacity Plans in UAE by ٢٠٠MW." November. https://www.datacenterdynamics.com/en/news/microsoft–/and–g٤٢–expand–data–center–capacity–plans–in–uae–by–٢٠٠mw

.8 Data Center Dynamics. ٢٠٢٥b. “Microsoft to Develop Azure Cloud Region in Kuwait.” March. https://www.datacenterdynamics.com/en/news/microsoft-to-develop-azure-cloud-region-in-kuwait/

.9 Data Center Dynamics. ٢٠٢٥c. “Ooredoo Launches AI Cloud in Qatar.” https://www.datacenterdynamics.com/en/news/ooredoo-launches-ai-cloud-in-qatar/

.10 Data Center World Middle East. ٢٠٢٦. “The Strategic Case for UAE Data Centre Investment.” https://www.datacenterworldmiddleeast.com/the-strategic-case-for-uae-data-centre-investment/

.11 DLA Piper. n.d. “Data Protection Laws in Bahrain.” Personal Data Protection Law No. ٣٠ of ٢٠١٨, in force August ١, ٢٠١٩. https://www.dlapiperdataprotection.com/index.html?t=law&c=BH

.12 Duane Morris & Selvam. ٢٠٢٦. “Singapore’s Digital & AI Governance: A Pro-Innovation, Framework-Driven Model.” Lexology. https://www.lexology.com/library/detail.aspx?g=٧٣٢b١٨f٠-b٠d٤-٤٥٣٦-٨٧٠٩-٨ac٩fed٨١bd٠

.13 European Insurance and Occupational Pensions Authority (EIOPA). n.d. “Digital Operational Resilience Act (DORA).” https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

.14 Foreign Policy / FP Analytics. ٢٠٢٢. “Why China’s New Data Security Law Is a Warning for the Future of Data Governance.” https://foreignpolicy.com/٢٠٢٢/٠١/٢٨/china-data-governance-security-law-privacy/

.15 Government Communications Office, State of Qatar. ٢٠٢٤. “The National Cyber Security Strategy ٢٠٢٤–٢٠٣٠ Is Launched.” September. https://www.gco.gov.qa/en/media-centre/top-news/the-national-cyber-security-strategy-٢٠٢٤-٢٠٣٠-is-launched/

16. Hogan Lovells. ٢٠٢٥. “India’s Digital Personal Data Protection Act ٢٠٢٣ Brought into Force.” November. https://www.hoganlovells.com/en/publications/indias-digital-personal-data-protection-act-٢٠٢٣-brought-into-force

17. Information Technology and Innovation Foundation (ITIF). n.d. “The ٢٠٢١ China Cloud Market.” https://www٢.itif.org/٢٠٢١-china-cloud-market.pdf

18. International Association of Privacy Professionals (IAPP). n.d. “The Personal Data Protection Framework in Singapore.” https://iapp.org/news/a/the-personal-data-protection-framework-in-singapore

19. Ministry of Communications and Information Technology (Saudi Arabia). n.d. “Saudi Arabia Expands Plan to Develop Digital Infrastructure to Build and Enable Mega Data Centers.” https://www.mcit.gov.sa/en/news/saudi-arabia-expands-plan-develop-digital-infrastructure-build-and-enable-mega-data-centers

20. NEOM. ٢٠٢٥. “DataVolt and NEOM to Develop Region’s First Net-Zero AI Factory.” February ١٠. https://www.neom.com/en-us/newsroom/datavolt-signs-agreement-with-neom

21. The Next Web. ٢٠٢٦. “Europe’s Cloud Dependency Is a Political Risk, Not Just a Technical One.” https://thenextweb.com/news/europes-cloud-dependency-political-risk

22. OpenAI. ٢٠٢٥. “Introducing Stargate UAE.” May. https://openai.com/index/introducing-stargate-uae/

23. ResearchAndMarkets. ٢٠٢٥. “GCC Data Center Market – Investment Analysis & Growth Opportunities ٢٠٢٥–٢٠٣٠.” March. https://www.globenewswire.com/news-release/٢٠٢٥/٠٣/١٣/٣٠٤٢٤٢٢/٢٨١٢٤/en/GCC-Data-Center-Market-Investment-Analysis-Report-٢٠٢٥-٢٠٣٠-Saudi-Arabia-and-UAE-Drive-GCC-Data-Center-Boom-with-٩-٤٩-Billion-Market-by-٢٠٣٠.html

24. Saudi Central Bank (SAMA). n.d. “SAMA Hosts ٧٩th Meeting of GCC Committee for Central Banks Governors.” https://www.sama.gov.sa/en-us/mediacenter/news/pages/news-٧٨٥.aspx

25. Saudi Data & Artificial Intelligence Authority (SDAIA) and National Data Management Office. ٢٠٢١. Personal Data Protection Law. Royal Decree M/١٩ of ٢٠٢١. See DataGuidance, “Saudi Arabia.” https://www.dataguidance.com/jurisdictions/saudi-arabia

26. Sophia, M. ٢٠٢٥. “How Stargate UAE Outsizes the World’s Largest Data Centres.” The National, May. https://www.thenationalnews.com/future/technology/٢٠٢٥/٠٥/٢٤/stargate-uae-ai-g٤٢/

27. Telecommunications Regulatory Authority (Oman). ٢٠٢٤. Ministerial Decision No. ١١٥٢/٢/١٩/٢٠٢٤-٢٠ on Cloud Computing and Data Centre Services. September. Analysis via Mondaq. https://www.mondaq.com/data-protection/١٥٤٣٥٠/navigating-the-new-telecommunications-regulatory-authority-tra-regulations-on-cloud-computing-and-data-centres-in-oman-legal-implications-and-subscriber-challenges

28. Uptime Institute. ٢٠٢٤. “Uptime Institute Launches Data Center Academy in Kingdom of Saudi Arabia.” March. https://uptimeinstitute.com/about-ui/press-releases/uptime-institute-launches-data-center-academy-in-kingdom-of-saudi-arabia

29. U.S. Congressional Research Service. ٢٠١٨. “Law Enforcement Access to Overseas Data Under the CLOUD Act.” LSB١٠٢٥. Washington, DC: Library of Congress. CLOUD Act ٢٠١٨, ١٨ U.S.C. § ٢٧١٣. https://www.congress.gov/crs-product/LSB١٠٢٥

30. World Bank. n.d. “Research and Development Expenditure (% of GDP).” https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS

31. World Economic Forum. ٢٠٢٥. “What Is Digital Sovereignty and How Are Countries Approaching It?” January. https://www.weforum.org/stories/٢٠٢٥/٠١/europe-digital-sovereignty/

مركز الخليج للأبحاث

المعرفة للجميع

Gulf Research Center

Knowledge for All